

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-20956

(43) 公開日 平成10年(1998) 1月23日

(51) Int.Cl. ⁹	識別記号	片内整理番号	F I	技術表示箇所
G 0 6 F 1/00	3 7 0		G 0 6 F 1/00	3 7 0 F
	5 5 0		9/06	5 5 0 A
				5 5 0 Z
13/00	3 5 1		13/00	3 5 1 E
G 0 9 C 1/00	6 3 0	7259-5 J	G 0 9 C 1/00	6 3 0 B

審査請求 未請求 請求項 23 O L (全 26 頁) 最終頁に続く

(21) 出願番号 特願平8-170106

(22) 出願日 平成8年(1996) 6月28日

(71) 出願人 000004226

日本電信電話株式会社

東京都新宿区西新宿三丁目19番2号

(72) 発明者 田中 利治

東京都新宿区西新宿三丁目19番2号 日本

電信電話株式会社内

(74) 代理人 弁理士 伊京 忠彦

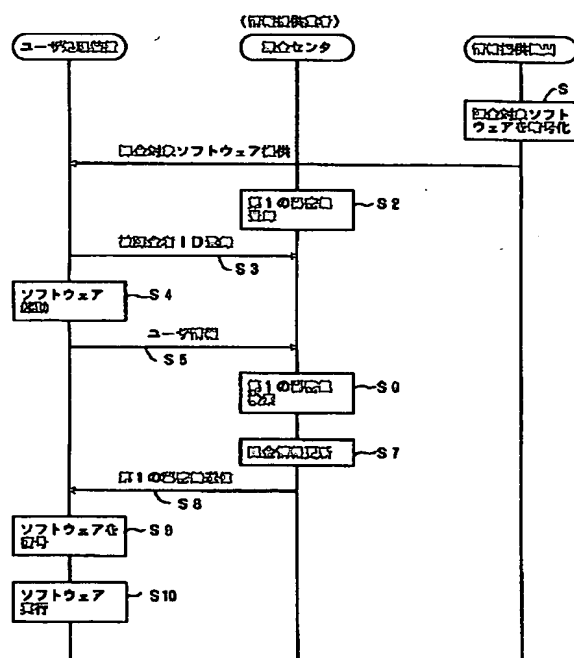
(54) 【発明の名称】 ソフトウェア課金方法及びシステム

(57) 【要約】

【課題】 ソフトウェアの使用機能に対応し、使用回数に比例した使用量の徴収を可能にするソフトウェア課金方法及びシステムを提供することを目的とする。

【解決手段】 被課金者がソフトウェアを起動し、ユーザ情報を課金センタに送信すると、課金センタはソフトウェアの使用料及び第1の復号・秘密鍵を検索することにより取得し、被課金者IDに対応する課金情報を更新し、取得した第1の復号・秘密鍵をユーザ処理装置に送信し、ユーザ処理装置は、課金センタから受信した第1の復号・秘密鍵を用いてソフトウェアの全部または、一部の暗号化されている領域を復号し、実行する。

本発明の図を説明するための図



1

【特許請求の範囲】

【請求項1】 ユーザ処理装置に提供するソフトウェアに対する使用料を課金するためのソフトウェア課金方法において、

情報提供機関は、

被課金者に提供するソフトウェアの全部または、一部を暗号化してユーザに配付し、

課金センタは、

課金対象ソフトウェア毎に、登録情報として、ソフトウェア識別子、ソフトウェア使用料、及び暗号化されたソフトウェアを復号するための第1の復号・秘密鍵を登録しておき、

前記被課金者は、前記課金センタに被課金者IDを登録しておき、

前記被課金者がソフトウェアを起動して、該ソフトウェアIDを含む該ソフトウェア使用通知を前記課金センタに送信すると、

前記課金センタは、前記ソフトウェア使用通知に基づいて前記ソフトウェアの使用料及び前記第1の復号・秘密鍵を検索し、

前記ソフトウェア使用料で前記被課金者IDに対応する課金情報を更新し、

取得した前記第1の復号・秘密鍵をユーザ処理装置に送信し、

前記ユーザ処理装置は、前記課金センタから受信した前記第1の復号・秘密鍵を用いて前記ソフトウェアの全部または、一部の暗号化されている領域を復号し、実行することを特徴とするソフトウェア課金方法。

【請求項2】 前記ユーザ処理装置は、

乱数を生成し、前記課金センタに、前記ソフトウェア使用通知と共に送信し、

前記課金センタは、

前記ユーザ処理装置から乱数を受信し、前記第1の復号・秘密鍵と共に受信した乱数を前記ユーザ処理装置に送信し、

前記ユーザ処理装置は、

前記課金センタから前記第1の復号・秘密鍵と前記乱数を受信し、

生成した前記乱数と受信した乱数とを比較し、一致するかを判定し、一致する場合のみ前記ソフトウェアの復号を行う請求項1記載のソフトウェア課金方法。

【請求項3】 前記課金センタにおいて、

前記登録情報として、前記ソフトウェアに対応する前記第1の復号・秘密鍵を暗号化するための第2の秘密鍵を更に含み、前記第2の秘密鍵を用いて、前記ユーザ処理装置に送信する前記第1の復号・秘密鍵を暗号化した暗号化情報を前記ユーザ処理装置に送信し、

前記ユーザ処理装置では、

前記ソフトウェアに埋め込んである第2の秘密鍵を抽出し、

2

前記第2の秘密鍵を用いて、前記暗号化情報を復号して前記第1の復号・秘密鍵を取得し、

取得した前記第1の復号・秘密鍵を用いて前記ソフトウェアを復号する請求項1又は、2記載のソフトウェア課金方法。

【請求項4】 前記ユーザ処理装置は、

被課金者の第3の私的秘密鍵を用いて、前記課金センタに送信する情報の一部を暗号化することにより署名を生成して、前記課金センタに送信し、

10 前記課金センタは、

前記登録情報として、更に被課金者の第3の私的秘密鍵に対応した公開鍵を含み、前記署名を該公開鍵で復号した情報と、前記ユーザ処理装置から受信した他の情報と一致しているかを判定し、

一致する場合のみ前記第1の復号・秘密鍵を前記ユーザ処理装置に送信する請求項1、2、又は、3記載のソフトウェア課金方法。

【請求項5】 前記ユーザ処理装置では、

20 暗号化された前記ソフトウェアを復号して、実行する際に、命令フェッチ及びオペランド・フェッチによるメモリ・アクセスの度に、メモリから読み出した暗号化データを復号して使用する請求項1、2、3、又は4記載のソフトウェア課金方法。

【請求項6】 前記ユーザ処理装置では、

前記暗号化されたソフトウェアを復号して実行する際に、

予め、復号したデータを格納するための領域を確保し、前記ソフトウェアの実行開始時または、実行中に、前記暗号化されたソフトウェアの全部または、一部を復号して、前記復号したデータを格納する領域に格納し、前記ソフトウェアの実行中の復号対象領域へのアクセスは、前記復号したデータを格納する領域へのアクセスで代替する請求項1、2、3又は4記載のソフトウェア課金方法。

【請求項7】 前記ユーザ処理装置は、

前記課金センタに、前記ソフトウェアの機能IDを前記ソフトウェア使用通知に付加して送信し、

前記課金センタは、

課金対象ソフトウェア毎に、ソフトウェアID、機能に対応した機能ID、機能に対応した使用料及び機能に対応した前記ソフトウェアを復号するための第4の復号・秘密鍵を登録情報として登録しておき、

前記ユーザ処理装置から送信された前記ソフトウェアID、及び前記機能IDを用いて、前記登録情報を検索し、機能使用料及び、前記第4の復号・秘密鍵を取得し、

前記被課金者ID、及び前記機能使用料を用いて、前記ユーザ情報を検索して、該被課金者IDに対応した課金情報を更新する請求項1、2、3、4、5又は、6記載のソフトウェア課金方法。

3

【請求項8】 前記情報提供機関が、ユーザに提供するソフトウェアの一部を暗号化する際に、前記ソフトウェアのアドレス範囲内のデータを暗号化する請求項1記載のソフトウェア課金方法。

【請求項9】 前記情報提供機関が、ユーザに提供するソフトウェアの一部を暗号化する際に、前記ソフトウェアの機能単位で暗号化する請求項1記載のソフトウェア課金方法。

【請求項10】 前記情報提供機関が、ユーザに提供するソフトウェアの一部を暗号化する際に、前記ソフトウェアの暗号化対象領域全ての一種類の秘密鍵で暗号化する請求項1記載のソフトウェア課金方法。

【請求項11】 前記情報提供機関が、ユーザに提供するソフトウェアの一部を暗号化する際に、前記ソフトウェアの暗号化対象領域を複数の副領域に分割し、分割された各々の副領域を異なる秘密鍵で暗号化する請求項10記載のソフトウェア課金方法。

【請求項12】 提供されたソフトウェアを使用するユーザ処理装置と、該ユーザ処理装置が使用するソフトウェアについて課金処理を行う課金センタと、該ユーザ処理装置及び該課金センタを接続するネットワークからなるソフトウェア課金システムであって、

前記ユーザ処理装置に対して提供するソフトウェアを第1の復号・秘密鍵を用いて暗号化する第1の暗号化手段と、

暗号化されたソフトウェアを前記ユーザ処理装置に提供するソフトウェア提供手段とを有する情報提供機関を含み、

前記課金センタは、

前記ユーザ処理装置から受信したソフトウェア使用通知に基づいて、該ユーザ処理装置が使用するソフトウェアに対する課金を行う課金手段と、

前記課金処理が終了した時点で、前記第1の暗号化手段で用いられた前記第1の復号・秘密鍵を前記ユーザ処理装置に送信する復号鍵送信手段とを有し、

前記ユーザ処理装置は、

予め、前記課金センタに対して自装置IDを登録するID登録手段と、

配付されたソフトウェアを使用するソフトウェア使用通知を前記課金センタに通知する使用通知手段と、

前記課金センタから受信した前記第1の復号秘密鍵を用いて、前記ソフトウェア全部、または、一部の暗号化されている領域を復号し、実行する第1の復号手段とを有することを特徴とするソフトウェア課金システム。

【請求項13】 前記課金センタの前記課金手段は、課金対象となるソフトウェア毎に、ソフトウェアID、ソフトウェア使用料、及び暗号化されたソフトウェアを復号するための第1の復号・秘密鍵を格納するための課金情報記憶手段と、

4

前記ユーザ毎に、被課金者ID及び、ユーザ課金情報を保持するユーザ情報記憶手段と、

前記ソフトウェアIDを用いて、前記課金情報記憶手段を検索して、ソフトウェア使用料、及び第1の復号・秘密鍵を取得する第1の検索手段と、

前記ユーザ処理装置から前記使用通知手段により送信された被課金者IDに基づいて前記ユーザ情報記憶手段を検索し、該被課金者IDに対応するユーザ課金情報を取得して、前記ソフトウェア使用料で更新する第1の課金情報更新手段とを含む請求項12記載のソフトウェア課金システム。

【請求項14】 前記ユーザ処理装置の前記通知手段は、

乱数を生成する乱数生成手段と、

前記課金センタに、前記ソフトウェア使用通知と共に、前記乱数生成手段で生成された乱数を送信する乱数送信手段とを含み、

前記第1の復号手段は、

前記課金センタから受信する乱数と前記乱数生成手段で生成された乱数とを比較し、一致するかを判定し、一致するときのみ復号を行う乱数判定手段とを含み、

前記課金センタの前記復号鍵送信手段は、前記乱数送信手段により前記ユーザ処理装置から受信した前記乱数を前記第1の復号・秘密鍵と共に送信する乱数送信手段を含む請求項12又は13記載のソフトウェア課金システム。

【請求項15】 前記課金センタの前記課金情報記憶手段は、

前記ソフトウェアに対応する前記第1の復号・秘密鍵を暗号化するための第2の秘密鍵を更に含み、

前記復号鍵送信手段は、

前記第2の秘密鍵を用いて、前記ユーザ処理装置に送信する前記第1の復号・秘密鍵を暗号化した暗号化情報を生成する第2の暗号化手段を含み、

前記ユーザ処理装置の第1の復号手段は、

前記課金センタから受信した前記暗号化情報を、前記ソフトウェアに埋め込んである第2の秘密鍵を抽出し、前記暗号化情報を該第2の秘密鍵で復号して、該第1の復号・秘密鍵を取得し、該第1の復号・秘密鍵で前記ソフトウェアを復号する第2の復号化手段を含む請求項12、13又は、14記載のソフトウェア課金システム。

【請求項16】 前記ユーザ処理装置の使用通知手段は、

被課金者の第3の私的秘密鍵を用いて、前記課金センタに送信するソフトウェア使用通知の一部を暗号化することにより署名を生成する署名生成手段と、

前記課金センタに送信する前記ソフトウェア使用通知と共に署名を前記課金センタに送信する署名送信手段を更に有し、

50 前記課金センタは、

前記ユーザ情報記憶手段に、被課金者の第3の私的秘鍵に対応した公開鍵を含み、

前記ユーザ情報記憶手段上の前記被課金者の第3の私的秘鍵に対応し、署名を復号するための公開鍵を用いて、前記ユーザ処理装置から受信した前記署名を復号し、該ユーザ処理装置から受信した前記ソフトウェア使用通知との一致を判定するユーザ情報判定手段を更に有する請求項12、13、14又は15記載のソフトウェア課金システム。

【請求項17】 前記第1の復号化手段は、命令フェッチ及びオペランド・フェッチによるメモリ・アクセスの度に、メモリから読み出した暗号化データを復号化して使用する手段を含む請求項12、13、14、15又は16記載のソフトウェア課金システム。

【請求項18】 前記第1の復号化手段は、予め復号したデータを格納する復号データ格納手段と、前記ソフトウェアの実行開始時、または、実行中に、暗号化されたソフトウェアの全部または、一部を復号して前記復号データ格納手段に格納し、該ソフトウェアの実行中の復号対象領域へのアクセスは、前記復号データ格納手段へのアクセスで代替する代替アクセス手段を含む請求項12、13、14、15又は16記載のソフトウェア課金システム。

【請求項19】 前記課金センタは、課金対象ソフトウェア毎に、ソフトウェアID、機能に対応した機能ID、機能に対応した使用料及び機能に対応し、前記ユーザ処理装置に送信され、該課金対象ソフトウェアを復号するための第4の復号・秘鍵を格納する第2の課金情報記憶手段と、前記ソフトウェアID及び前記機能IDを用いて、前記第2の課金情報記憶手段を検索して、機能使用料及び第4の復号・秘鍵を取得する第2の検索手段と、前記被課金者ID及び前記機能使用料を用いて、前記ユーザ情報記憶手段を検索して、前記被課金者IDに対応したユーザ課金情報を更新する第2の課金情報更新手段を更に有し、前記ユーザ処理装置は、被課金者ID及びソフトウェアIDと共に、機能IDを前記課金センタに送信するID通知手段を更に有する請求項12、13、14、15、16、17または、18記載のソフトウェア課金システム。

【請求項20】 前記情報提供機関の前記第1の暗号化手段は、前記ソフトウェアのアドレス範囲内のデータを暗号化する手段を含む請求項12記載のソフトウェア課金システム。

【請求項21】 前記情報提供機関の前記第1の暗号化手段は、前記ソフトウェアの機能単位で暗号化する手段を含む請求項12記載のソフトウェア課金システム。

【請求項22】 前記情報提供機関の前記第1の暗号化手段は、

前記ソフトウェアの暗号化対象領域全ての一種類の秘鍵で暗号化する手段を含む請求項12記載のソフトウェア課金システム。

【請求項23】 前記情報提供機関の前記第1の暗号化手段は、

前記ユーザ処理装置に提供するソフトウェアの一部を暗号化する際に、前記ソフトウェアの暗号化対象領域を複数の副領域に分割し、分割された各々の副領域を異なる秘鍵で暗号化する手段を含む請求項22記載のソフトウェア課金システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ソフトウェア課金方法及びシステムに係り、特に、CD-ROMやフロッピーディスク等の媒体に格納されて配付されるソフトウェアや、ネットワークを介して配付されるソフトウェアに対して課金を行うソフトウェア課金方法及びシステムに関する。

【0002】

【従来の技術】従来のソフトウェア課金システムには、ソフトウェアを販売し、ユーザが当該ソフトウェアを買い取られた時点で課金が終了する方法がある。また、ユーザが配付されたソフトウェアを使用する際に、課金センタに使用する旨を通知し、これにより、課金センタでは、ソフトウェアの使用に対する課金を行うシステムがある。

【0003】また、最近では、買い取り形式の変形として暗号化されたソフトウェアをCD-ROM等の媒体または、ネットワーク経由で配付し、電話、ファクシミリ、手紙または、電子メールによる購入手続き後、復号鍵を通知する方式も採用されている。さらに、予め利用可能量が設定され、かつ、暗号化されたソフトウェアを配付して、ユーザが使用した量を日数で管理し、当該日数に基づいて課金を行う方法等がある。

【0004】

【発明が解決しようとする課題】しかしながら、上記の買い取り方式では、流通経費を相対的に低減するためにソフトウェアの機能は肥大化し、ユーザは、殆ど使用しない機能を含め、高額のコストを負担しなければならない。また、ソフトウェアを購入して実行してみなければユーザが必要とする機能が満足されているか否かを判断できない。

【0005】また、単に、ユーザが配付されたソフトウェアを使用する際に、課金センタに使用する旨を通知する方法では、課金は可能であってもソフトウェアの使用を制限することができないため、使用料金の未払いがあっても対処することができないという問題がある。

【0006】暗号化されたソフトウェアを予め提供し、

使用時に復号鍵を提供するシステムであっても、使用回数に関わらず、ユーザは、同一の金額を支払う必要があり、使用回数または、使用時間当たりの価格には大きな幅がある。本発明は、上記の点に鑑みなされたもので、ソフトウェアの使用機能に対応し、使用回数に比例した使用量の徴収を可能にするソフトウェア課金方法及びシステムを提供することを目的とする。

【0007】詳しくは、ソフトウェアの使用要求に対して、ユーザ課金情報を更新した後、使用許可を与え、使用許可されたソフトウェアがただ1回だけ使用可能であることを保障し、1回当たりの使用料を安価にすることが可能なソフトウェア課金方法及びシステムを提供することである。

【0008】

【課題を解決するための手段】図1は、本発明の原理を説明するための図である。本発明は、ユーザ処理装置に提供するソフトウェアに対する使用料を課金するためのソフトウェア課金方法において、情報提供機関は、被課金者に提供するソフトウェアの全部または、一部を暗号化してユーザに配付し（ステップ1）、課金センタは、課金対象ソフトウェア毎に、登録情報として、ソフトウェア識別子、ソフトウェア使用料及び暗号化されたソフトウェアを復号するための第1の復号・秘密鍵を登録しておき（ステップ2）、被課金者は、課金センタに被課金者IDを登録しておき（ステップ3）、被課金者がソフトウェアを起動して（ステップ4）、該ソフトウェアIDを含む該ソフトウェア使用通知を課金センタに送信すると（ステップ5）、課金センタは、ソフトウェア使用通知に基づいてソフトウェアの使用料及び第1の復号・秘密鍵を検索し（ステップ6）、ソフトウェア使用料で被課金者IDに対応する課金情報を更新し（ステップ7）、取得した第1の復号・秘密鍵をユーザ処理装置に送信し（ステップ8）、ユーザ処理装置は、課金センタから受信した第1の復号・秘密鍵を用いてソフトウェアの全部または、一部の暗号化されている領域を復号し（ステップ9）、実行する（ステップ10）。

【0009】また、本発明において、ユーザ処理装置は、乱数を生成し、課金センタに、ソフトウェア使用通知と共に送信し、課金センタは、ユーザ処理装置から乱数を受信し、第1の復号・秘密鍵と共に受信した乱数をユーザ処理装置に送信し、ユーザ処理装置は、課金センタから第1の復号・秘密鍵と乱数を受信し、生成した乱数と受信した乱数とを比較し、一致するかを判定し、一致する場合のみソフトウェアの復号を行う。

【0010】また、本発明は、課金センタにおいて、登録情報として、ソフトウェアに対応する第1の復号・秘密鍵を暗号化するための第2の秘密鍵を更に含み、第2の秘密鍵を用いて、ユーザ処理装置に送信する第1の復号・秘密鍵を暗号化した暗号化情報をユーザ処理装置に送信し、ユーザ処理装置では、ソフトウェアに埋め込ん

である第2の秘密鍵を抽出し、第2の秘密鍵を用いて、暗号化情報を復号して第1の復号・秘密鍵を取得し、取得した第1の復号・秘密鍵を用いてソフトウェアを復号する。

【0011】また、本発明において、ユーザ処理装置は、被課金者の第3の私的秘密鍵を用いて、課金センタに送信する情報の一部を暗号化することにより署名を生成して、課金センタに送信し、課金センタは、登録情報として、更に被課金者の第3の私的秘密鍵に対応した公開鍵を含み、署名を該公開鍵で復号した情報と、ユーザ処理装置から受信した他の情報と一致しているかを判定し、一致する場合のみ第1の復号・秘密鍵をユーザ処理装置に送信する。

【0012】また、本発明において、ユーザ処理装置では、暗号化されたソフトウェアを復号して、実行する際に、命令フェッチ及びオペランド・フェッチによるメモリ・アクセスの度に、メモリから読み出した暗号化データを復号して使用する。

【0013】また、本発明において、ユーザ処理装置では、暗号化されたソフトウェアを復号して実行する際に、予め、復号したデータを格納するための領域を確保し、ソフトウェアの実行開始時または、実行中に、暗号化されたソフトウェアの全部または、一部を復号して、復号したデータを格納する領域に格納し、ソフトウェアの実行中の復号対象領域へのアクセスは、復号したデータを格納する領域へのアクセスで代替する。

【0014】また、本発明において、ユーザ処理装置は、課金センタに、ソフトウェアの機能IDをソフトウェア使用通知に付加して送信し、課金センタは、課金対象ソフトウェア毎に、ソフトウェアID、機能に対応した機能ID、機能に対応した使用料及び機能に対応したソフトウェアを復号するための第4の復号・秘密鍵を登録情報として登録しておき、ユーザ処理装置から送信されたソフトウェアID、及び機能IDを用いて、登録情報を検索し、機能使用料及び、第4の復号・秘密鍵を取得し、被課金者ID、及び機能使用料を用いて、ユーザ情報を検索して、該被課金者IDに対応した課金情報を更新する。

【0015】また、本発明は、情報提供機関が、ユーザに提供するソフトウェアの一部を暗号化する際に、ソフトウェアのアドレス範囲内のデータを暗号化する。また、本発明は、情報提供機関が、ユーザに提供するソフトウェアの一部を暗号化する際に、ソフトウェアの機能単位で暗号化する。

【0016】また、本発明は、情報提供機関が、ユーザに提供するソフトウェアの一部を暗号化する際に、ソフトウェアの暗号化対象領域全ての一種類の秘密鍵で暗号化する。また、本発明は、情報提供機関が、ユーザに提供するソフトウェアの一部を暗号化する際に、ソフトウェアの暗号化対象領域を複数の副領域に分割し、分割さ

れた各々の副領域を異なる秘密鍵で暗号化する。

【0017】図2は、本発明の原理構成図である。本発明は、提供されたソフトウェアを使用するユーザ処理装置100と、該ユーザ処理装置100が使用するソフトウェアについて課金処理を行う課金センタ200と、該ユーザ処理装置100及び該課金センタ200を接続するネットワークからなるソフトウェア課金システムであって、ユーザ処理装置100に対して提供するソフトウェアを第1の復号・秘密鍵を用いて暗号化する第1の暗号化手段と、暗号化されたソフトウェアをユーザ処理装置100に提供するソフトウェア提供手段とを有する情報提供機関を含み、課金センタ200は、ユーザ処理装置100から受信したソフトウェア使用通知に基づいて、該ユーザ処理装置100が使用するソフトウェアに対する課金を行う課金手段240と、課金処理が終了した時点で、第1の暗号化手段で用いられた第1の復号・秘密鍵をユーザ処理装置100に送信する復号鍵送信手段250とを有し、ユーザ処理装置100は、予め、課金センタ200に対して自装置IDを登録するID登録手段101と、配付されたソフトウェアを使用するソフトウェア使用通知を課金センタ200に通知する使用通知手段120と、課金センタ200から受信した第1の復号秘密鍵を用いてソフトウェアの全部または、一部暗号化された領域を復号し、実行する第1の復号手段130とを有する。

【0018】また、本発明において、課金センタ200の課金手段240は、課金対象となるソフトウェア毎に、ソフトウェアID、ソフトウェア使用料、及び暗号化されたソフトウェアを復号するための第1の復号・秘密鍵を格納するための課金情報記憶手段と、ユーザ毎に、被課金者ID及び、ユーザ課金情報を保持するユーザ情報記憶手段と、ソフトウェアIDを用いて、課金情報記憶手段を検索して、ソフトウェア使用料、及び第1の復号・秘密鍵を取得する第1の検索手段と、ユーザ処理装置100から使用通知手段120により送信された被課金者IDに基づいてユーザ情報記憶手段を検索し、該被課金者IDに対応するユーザ課金情報を取得して、ソフトウェア使用料で更新する第1の課金情報更新手段とを含む。

【0019】また、本発明のユーザ処理装置100の通知手段は、乱数を生成する乱数生成手段と、課金センタ200に、ソフトウェア使用通知と共に、乱数生成手段で生成された乱数を送信する乱数送信手段とを含み、第1の復号手段130は、課金センタ200から受信する乱数と乱数生成手段で生成された乱数とを比較し、一致するかを判定し、一致するときのみ復号を行う乱数判定手段とを含み、課金センタ200の復号鍵送信手段250は、乱数送信手段によりユーザ処理装置100から受信した乱数を第1の復号・秘密鍵と共に送信する乱数送信手段を含む。

【0020】また、本発明の課金センタ200の課金情報記憶手段は、ソフトウェアに対応する第1の復号・秘密鍵を暗号化するための第2の秘密鍵を更に含み、復号鍵送信手段250は、第2の秘密鍵を用いて、ユーザ処理装置100に送信する第1の復号・秘密鍵を暗号化した暗号化情報を生成する第2の暗号化手段を含み、ユーザ処理装置100の第1の復号手段130は、課金センタ200から受信した暗号化情報を、ソフトウェアに埋め込んである第2の秘密鍵を抽出し、暗号化情報を復号して第1の復号・秘密鍵を取得し、該第1の復号・秘密鍵でソフトウェアを復号する第2の復号化手段を含む。

【0021】また、本発明のユーザ処理装置100の使用通知手段120は、被課金者の第3の私的秘密鍵を用いて、課金センタ200に送信するソフトウェア使用通知の一部を暗号化することにより署名を生成する署名生成手段と、課金センタ200に送信するソフトウェア使用通知と共に署名を課金センタ200に送信する署名送信手段を更に有し、課金センタ200は、ユーザ情報記憶手段に、被課金者の第3の私的秘密鍵に対応した公開鍵を含み、ユーザ情報記憶手段上の被課金者の第3の私的秘密鍵に対応し、署名を復号するための公開鍵を用いて、ユーザ処理装置100から受信した署名を復号し、該ユーザ処理装置100から受信したソフトウェア使用通知との一致を判定するユーザ情報判定手段を更に有する。

【0022】また、本発明の第1の復号化手段は、命令フェッチ及びオペランド・フェッチによるメモリ・アクセスの度に、メモリから読み出した暗号化データを復号化して使用する手段を含む。また、本発明の第1の復号化手段は、予め復号したデータを格納する復号データ格納手段と、ソフトウェアの実行開始時、または、実行中に、暗号化されたソフトウェアの全部または、一部を復号して復号データ格納手段に格納し、該ソフトウェアの実行中の復号対象領域へのアクセスは、復号データ格納手段へのアクセスで代替する代替アクセス手段を含む。

【0023】また、本発明の課金センタ200は、課金対象ソフトウェア毎に、ソフトウェアID、機能に対応した機能ID、機能に対応した使用料及び機能に対応し、ユーザ処理装置100に送信され、該課金対象ソフトウェアを復号するための第4の復号・秘密鍵を格納する第2の課金情報記憶手段と、ソフトウェアID及び機能IDを用いて、第2の課金情報記憶手段を検索して、機能使用料及び第4の復号・秘密鍵を取得する第2の検索手段と、被課金者ID及び機能使用料を用いて、ユーザ情報記憶手段を検索して、被課金者IDに対応したユーザ課金情報を更新する第2の課金情報更新手段を更に有し、ユーザ処理装置100は、被課金者ID及びソフトウェアIDと共に、機能IDを課金センタ200に送信するID通知手段を更に有する。

【0024】また、本発明の情報提供機関の第1の暗号

化手段は、ソフトウェアのアドレス範囲内のデータを暗号化する手段を含む。また、本発明の情報提供機関の第1の暗号化手段は、ソフトウェアの機能単位で暗号化する手段を含む。

【0025】また、本発明の情報提供機関の第1の暗号化手段は、ソフトウェアの暗号化対象領域全ての一種類の秘密鍵で暗号化する手段を含む。また、本発明の情報提供機関の第1の暗号化手段は、ユーザ処理装置100に提供するソフトウェアの一部を暗号化する際に、ソフトウェアの暗号化対象領域を複数の副領域に分割し、分割された各々の副領域を異なる秘密鍵で暗号化する手段を含む。

【0026】上記の各発明では、予め、ユーザに提供するソフトウェアの全部または、一部が、当該ソフトウェアの開発時または、提供の前に暗号化されているものとする。このソフトウェアの一部を暗号化する場合には、あるアドレスの範囲内のデータを暗号化してもよいし、命令部、または、データ部を暗号化してもよいし、あるいは、機能の単位で暗号化してもよい。また、暗号化対象領域の全てを一種類の秘密鍵で暗号化してもよいし、暗号化対象領域を複数の副領域に分け、それぞれの副領域を異なる秘密鍵で暗号化してもよい。このように、種々の方法により暗号化が可能である。

【0027】また、本発明では、ソフトウェアの提供前に、課金センタの課金情報記憶手段に、ソフトウェアIDと、ソフトウェア使用料、及び上記の暗号化されたソフトウェアを復号するための秘密鍵を登録しておく。さらに、ユーザは、ソフトウェアの使用に先立ち、課金センタのユーザ情報テーブルに被課金者IDを登録しておく。

【0028】ユーザがユーザ処理装置上でソフトウェアを起動し、ソフトウェアの実行前または、実行中に、当該ユーザ処理装置から、ソフトウェアID及び被課金者IDを課金センタに送信すると、課金センタでは課金情報記憶手段を、ユーザ処理装置から受信したソフトウェアIDを用いて検索し、ソフトウェアの使用料及び復号するための秘密鍵を取得する。次に、課金センタのユーザ課金情報を、ユーザ処理装置から受信した被課金者IDを用いてユーザ情報記憶手段を検索し、課金情報テーブルから取得したソフトウェア使用料を用いて被課金者のユーザ課金情報を更新することにより、被課金者毎の課金処理を行う。さらに、課金センタは、ユーザ処理装置に課金情報記憶手段から取得した復号するための秘密鍵を送信する。これにより、ユーザ処理装置は、課金センタから受信した秘密鍵を用いて、ソフトウェアの全部または、一部の暗号化されている領域を復号して実行する。

【0029】これにより、情報提供機関から暗号化されたソフトウェアを提供し、ユーザが当該ソフトウェアを実行する（起動する）際に、課金センタにおいて課金処

理を行い、当該ソフトウェアを使用するための秘密鍵を送信することにより、ユーザに当該ソフトウェアの使用を許可する。

【0030】さらに、ソフトウェアの一部を暗号化して送信することにより、ユーザが全てのソフトウェアを利用しない場合に、ユーザは、使用しないソフトウェアに対する支払いを行う必要がない。また、本発明は、ユーザ処理装置において生成した乱数を課金センタに送信し、課金センタから返却された乱数とを照合して、一致する場合のみソフトウェアの復号を行うことにより、第三者の不正使用を防止する。

【0031】また、本発明は、ソフトウェアを復号するための第1の復号秘密鍵を更に暗号化した暗号化情報をユーザ処理装置に送信し、ユーザ処理装置では、当該暗号化情報を復号して取得した第1の復号鍵を用いて、ソフトウェアを復号して実行することにより、ユーザは、課金センタから受信した暗号化情報を復号できない限りソフトウェアを復号することができない。

【0032】また、本発明は、ユーザ処理装置において署名を生成して課金センタに送信し、課金センタにおいて、署名を復号した情報と受信した他の情報が一致しているかを判定し、不一致の場合にはユーザ処理装置に第1の復号秘密鍵を送信しないため、悪意の第三者が別の署名を送信した場合には、ソフトウェアを復号し、実行することができない。

【0033】また、本発明は、復号されたデータを格納する領域を設定しておくことにより、復号されたソフトウェアを順次当該領域に格納しておくことにより、実行時におけるソフトウェアのアクセスを当該領域に対して行うことにより、既に復号されているソフトウェアが格納されているため効率のよいアクセスが可能となる。

【0034】また、本発明は、ユーザ処理装置から課金センタにソフトウェアIDや被課金者IDと共に、ソフトウェアの機能IDを併せて送信することにより、起動するソフトウェア内の機能群単位に課金することが可能となる。

【0035】

【発明の実施の形態】図3は、本発明のシステム構成図である。以下に説明するシステムは、ユーザ処理装置100と課金センタ200及び当該ユーザ処理装置100と課金センタ200を接続する通信網（図示せず）から構成される。

【0036】なお、課金センタ200は、当該ソフトウェアを提供する情報提供者であり、課金システムを実行することから便宜的に課金センタと記すものとするが、情報提供者と課金センタは別個に独立して設定されていてもよい。ユーザ処理装置100は、課金センタ送信部120と復号部130とを有し、復号部130は、課金対象となるソフトウェア110を復号鍵（以下、第1の復号・秘密鍵）を用いて復号する。ソフトウェア1

10は、その全部または、一部が1つまたは、複数の秘密鍵を用いて暗号化されているものであり、予め課金センタ200（情報提供者）から提供されているものとする。

【0037】課金センタ送信部120は、自装置の被課金者ID等のユーザ情報及び起動するソフトウェアIDを送信する。課金センタ200は、課金情報テーブル210、ユーザ情報テーブル220、課金情報テーブル検索部230、ユーザ課金情報更新部240、ユーザ処理装置送信部250とを有する。

【0038】課金情報テーブル210は、ソフトウェアID、ソフトウェア使用料、暗号化されたソフトウェアを復号するための第1の復号秘密鍵から構成される。なお、以下の説明では、情報提供者から、予め、ユーザ処理装置100に配付するためのソフトウェアの全部または、一部を暗号化してユーザ処理装置100に送信し、暗号化時に使用した秘密鍵を第1の復号秘密鍵として、課金センタ200の課金情報テーブル210に登録しておくものとする。

【0039】ユーザ情報テーブル220は、ユーザ処理装置100から転送された被課金者IDと、ユーザ課金情報とから構成される。課金情報テーブル検索部230は、ユーザ処理装置100から受信したソフトウェアIDを用いて課金情報テーブル210を検索し、当該ソフトウェアの使用料を取得し、ユーザ課金情報更新部240に転送し、さらに、検索により、第1の復号秘密鍵を取得して、ユーザ処理装置送信部250に転送する。

【0040】ユーザ課金情報更新部240は、ユーザ処理装置100から受信した被課金者IDを用いてユーザ情報テーブル220を検索し、当該被課金者のユーザ課金情報を取得し、ソフトウェアの使用料で更新する。ユーザ処理装置送信部250は、課金情報テーブル検索部230から取得した第1の復号秘密鍵をユーザ処理装置100に転送する。

【0041】

【実施例】以下、図面と共に、本発明の実施例を詳細に説明する。

【第1の実施例】本実施例におけるシステム構成は、前述の図3に示すシステム構成によるものである。

【0042】図4は、本発明の第1の実施例の動作を説明するための図である。

ステップ101) ユーザ処理装置100は、予め、情報提供者から提供されたソフトウェア110を起動させる。

ステップ102) 当該ソフトウェア110をメモリ上にロードする。

【0043】ステップ103) ユーザ処理装置100において、予め暗号化されたソフトウェア110を起動すると、ユーザ処理装置100の課金センタ送信部120は、ソフトウェアIDと被課金者IDとを課金センタ

200に送信する。

ステップ104) 課金センタ200は、ユーザ処理装置100からソフトウェアIDと被課金者IDとを受信し、課金情報テーブル検索部230は、ソフトウェアIDを用いて課金情報テーブル210を検索し、当該ソフトウェアIDに対応するソフトウェアの使用料と、第1の復号秘密鍵とを取得する。

【0044】ステップ105) ユーザ課金情報更新部240は、受信した被課金者IDを用いて、ユーザ情報テーブル220を検索し、当該被課金者のユーザ課金情報を取得し、課金情報テーブル検索部230で検索されたソフトウェアの使用料を用いて、ユーザ課金情報を更新する（ソフトウェアの使用料をユーザ課金情報に加算する）。

【0045】ステップ106) ユーザ処理装置送信部250は、課金情報テーブル検索部230で検索された第1の復号秘密鍵をユーザ処理装置100に送信する。ステップ107) ユーザ処理装置100は、課金センタ200から受信した第1の復号秘密鍵を用いて、ソフトウェアの全部または、一部の暗号化されている領域を復号して実行する。

【0046】このように、本実施例によれば、ユーザ処理装置100からソフトウェア使用通知としてソフトウェアIDと被課金者IDを課金センタ200に送出することにより、課金センタからソフトウェアを復号するための第1の復号・秘密鍵を受け取り、暗号化されているソフトウェアを復号して実行することができる。

【0047】【第2の実施例】本実施例は、乱数を用いてソフトウェアの復号を許可することが可能か否かを判定する処理を前述の第1の実施例に付加したものである。図5は、本発明の第2の実施例のシステム構成図である。同図において、図3と同一構成部分には、同一符号を付し、その説明を省略する。

【0048】同図に示す構成は、前述の図3のシステム構成において、ユーザ処理装置100に乱数を生成する乱数生成部140と比較部150とを具備し、課金センタ200に乱数受信部260を具備する構成である。ユーザ処理装置100の乱数生成部140は、乱数を生成し、当該乱数を課金センタ送信部120に転送し、課金センタ送信部120から課金センタ200に送信する。比較部150は、課金センタ200から戻された乱数と、乱数生成部140で生成された乱数と課金センタ200から返却された乱数とを比較し、一致している場合に、復号部120に対してソフトウェア100の復号を許可する。

【0049】課金センタ200の乱数受信部260は、ユーザ処理装置100から取得した乱数をユーザ処理装置送信部250を介してユーザ処理装置100に戻す処理を行う。

【0050】図6は、本発明の第2の実施例の動作を説

明するための図である。

ステップ201) ユーザ処理装置100は、予め情報提供者から提供されたソフトウェア110を起動させる。

ステップ202) 当該ソフトウェア110をメモリ上にロードする。

【0051】ステップ203) 乱数生成部140は、乱数を生成し、課金センタ送信部120に転送する。

ステップ204) 課金センタ送信部120は、ソフトウェアIDと被課金者ID及び、乱数とを課金センタ200に送信する。

【0052】ステップ205) 課金センタ200において、乱数受信部260は、乱数を受信し、第1の実施例と同様に、ユーザ処理装置100からソフトウェアIDと被課金者IDを受信し、課金情報テーブル検索部230は、ソフトウェアIDを用いて課金情報テーブル210を検索し、当該ソフトウェアIDに対応するソフトウェアの使用料と、第1の復号秘密鍵とを取得する。

【0053】ステップ206) ユーザ課金情報更新部240は、受信した被課金者IDを用いて、ユーザ情報テーブル220を検索し、当該被課金者のユーザ課金情報を取得し、課金情報テーブル検索部230で検索されたソフトウェアの使用料を用いて、ユーザ課金情報を更新する(ソフトウェアの使用料をユーザ課金情報に加算する)。

【0054】ステップ207) ユーザ処理装置送信部250は、課金情報テーブル検索部230で検索された第1の復号秘密鍵と乱数受信部260で受信した乱数をユーザ処理装置100に送信する。

ステップ208) ユーザ処理装置100は、課金センタ200から受信した乱数とステップ203で生成された乱数とを比較し、一致する場合には、復号部130において、課金センタ200から受信した第1の復号秘密鍵を用いて、ソフトウェアの全部または、一部の暗号化されている領域を復号して実行する。

【0055】本実施例では、ユーザ処理層100から課金センタ200に送信した乱数と、課金センタ200から受信した乱数とが一致したときのみソフトウェアの復号を可能とする。

【第3の実施例】本実施例のシステム構成は、基本的に図3に示す構成と同様であるが、課金情報テーブル210において、第2の秘密鍵を保持し、課金情報テーブル検索部230においてソフトウェアIDに基づいて当該第2の秘密鍵を検索し、ユーザ課金情報更新部240において、第1の復号・秘密鍵を暗号化する点において異なる。

【0056】図7は、本発明の第3の実施例の動作を説明するための図である。

ステップ301) ユーザ処理装置100は、予め、情報提供者から提供されたソフトウェア110を起動さ

せる。

ステップ302) 当該ソフトウェア110をメモリ上にロードする。

【0057】ステップ303) 課金センタ送信部120は、ソフトウェアIDと被課金者IDを課金センタ200に送信する。

ステップ304) 課金センタ200は、ユーザ処理装置100からソフトウェアIDと被課金者IDを受信し、課金情報テーブル検索部230は、ソフトウェアIDを用いて課金情報テーブル210を検索し、当該ソフトウェアIDに対応するソフトウェアの使用料、第1の復号秘密鍵及び、第2の秘密鍵とを取得する。

【0058】ステップ305) ユーザ課金情報更新部240は、受信した被課金者IDを用いて、ユーザ情報テーブル220を検索し、当該被課金者のユーザ課金情報を取得し、課金情報テーブル検索部230で検索されたソフトウェアの使用料を用いて、ユーザ課金情報を更新する(ソフトウェアの使用料をユーザ課金情報に加算する)。

【0059】ステップ306) さらに、ユーザ課金情報更新部240は、第1の復号秘密鍵を課金情報テーブル210から取得した第2の秘密鍵を用いて暗号化し、ユーザ処理装置送信部250に転送する。

ステップ307) ユーザ処理装置送信部250は、ユーザ課金情報更新部240で暗号化された情報をユーザ処理装置100に送信する。

【0060】ステップ308) ユーザ処理装置100の復号部130は、課金センタ200から受信した暗号化された情報、ソフトウェア110に埋め込まれている第2の秘密鍵を用いて復号し、第1の復号秘密鍵を取得する。

ステップ309) さらに、復号部130は、ステップ308で復号することにより取得した第1の復号秘密鍵を用いて、ソフトウェアの全部または、一部の暗号化されている領域を復号して実行する。

【0061】このように、本実施例によれば、第1の復号・秘密鍵を暗号化してユーザ処理装置に送信することにより、より安全な第1の復号・秘密鍵を送信することができる。

【第4の実施例】図8は、本発明の第4の実施例のシステム構成図である。同図において、図3と同一構成部分には、同一符号を付し、その説明を省略する。

【0062】図8に示すシステムにおいて、図3と異なる構成は、ユーザ処理装置100においては、第3の私的秘密鍵保持部160と署名生成部170を含む点である。第3の私的秘密鍵保持部160は、署名を生成するための第3の私的秘密鍵を保持する。署名生成部170は、第3の私的秘密鍵を用いて署名を生成する。

【0063】また、課金センタ200のユーザ情報テーブル220は、被課金者ID、課金情報に加えて、署名

を復号するための公開鍵を保持する。図9は、本発明の第4の実施例のユーザ課金情報更新部の詳細な構成を示す。同図に示すユーザ課金情報更新部240は、ユーザ情報テーブルを検索し、公開鍵を取得するテーブル検索部241、ユーザ処理装置100から取得した署名を公開鍵を用いて復号する署名復号部242、ユーザ処理装置100から受信した他の情報と復号された情報とが一致しているかを比較する比較部243、ユーザ情報テーブル220を更新するテーブル更新部244から構成される。

【0064】テーブル更新部244は、比較部243において、復号化情報と、ユーザ処理装置100から受信した情報が一致している場合に限り、被課金者のユーザ課金情報を課金情報テーブル検索部230から取得したソフトウェア使用料で更新し、さらに、テーブル検索部241から取得した、第1の復号秘密鍵をユーザ処理装置送信部250に転送する。

【0065】図10は、本発明の第4の実施例の動作を説明するための図である。

ステップ401) ユーザ処理装置100は、予め、情報提供者から提供されたソフトウェア110を起動させる。

ステップ402) 当該ソフトウェア110をメモリ上にロードする。

【0066】ステップ403) ユーザ処理装置100の署名生成部170は、第3の私的秘密鍵保持部160から第3の私的秘密鍵を読み出して、ソフトウェアID、被課金者IDとの一部を当該第3の私的秘密鍵を用いて暗号化することにより、署名を生成し、課金センタ送信部120に転送する。

【0067】ステップ404) 課金センタ送信部120は、暗号化されたソフトウェアIDと被課金者IDを課金センタ200に送信する。

ステップ405) ユーザ課金情報更新部240のテーブル検索部241は、受信した暗号化情報に対して、ユーザ情報テーブル220を検索して公開鍵を取得して署名復号部242に転送する。署名復号部242は、当該被課金者の公開鍵を取得し、当該暗号化情報を公開鍵で復号し、比較部243に転送する。比較部243は、ユーザ処理装置100から受信した他の情報と比較し、一致しているかを判定する。一致している場合には、次のステップに移行する。

【0068】ステップ406) 課金センタ200の課金情報テーブル検索部230は、ユーザ処理装置100から受信したソフトウェアIDと被課金者IDを用いて、課金情報テーブル210を検索し、当該ソフトウェアIDに対応するソフトウェアの使用料、第1の復号秘密鍵とを取得する。

【0069】ステップ407) ユーザ課金情報更新部240のテーブル更新部244は、課金情報テーブル検

索部230からユーザ課金情報を取得し、課金情報テーブル検索部230で検索されたソフトウェアの使用料を用いて、ユーザ課金情報を更新する(ソフトウェアの使用料をユーザ課金情報に加算する)。

【0070】ステップ408) さらに、ユーザ課金情報更新部240は、第1の復号秘密鍵をユーザ処理装置送信部250に転送し、ユーザ処理装置送信部250は、ユーザ課金情報更新部240で暗号化された情報をユーザ処理装置100に送信する。

10 【0071】ステップ409) ユーザ処理装置100の復号部130は、第1の復号秘密鍵を用いてソフトウェアの全部または、一部の暗号化されている領域を復号して実行する。なお、本発明は、前述の各実施例と組み合わせることも可能である。これにより、署名と一致しない場合には、課金センタ200からユーザ処理装置100に第1の復号・秘密鍵を送信しないため、正当な署名を持たない限り、ユーザは、ソフトウェアを復号できない。

【0072】[第5の実施例] 本実施例におけるシステム構成は、図3と基本的に同様である。図11は、本発明の第5の実施例の動作を説明するための図である。

ステップ501) ユーザ処理装置100において、予め命令部分が暗号化されたソフトウェア110を起動する。

【0073】ステップ502) ユーザ処理装置100は、ソフトウェア100をロードする。

ステップ503) ユーザ処理装置100の課金センタ送信部120は、ソフトウェアID、被課金者IDとを課金センタ200に送信する。

30 【0074】ステップ504) 課金センタ200の課金情報テーブル検索部230は、ユーザ処理装置100から受信したソフトウェアIDを用いて課金情報テーブル210を検索し、当該ソフトウェアの使用料と、第1の復号秘密鍵とを取得する。

ステップ505) ユーザ課金情報更新部240は、ユーザ処理装置100から受信した被課金者IDを用いてユーザ情報テーブル220を検索し、被課金者のユーザ課金情報を課金情報テーブル210から取得したソフトウェア使用料で更新する。

40 【0075】ステップ506) ユーザ処理装置送信部250は、課金情報テーブル検索部230から取得した第1の復号秘密鍵をユーザ処理装置100に送信する。ステップ507) ユーザ処理装置100の復号部130は、課金センタ200から受信した第1の復号秘密鍵を用いて、次に実行する命令を読み出す。

【0076】ステップ508) 復号部130は、読み出した命令を復号する。

ステップ509) 復号部130により復号された命令を実行する。

50 ステップ508とステップ509の処理を当該復号され

た命令の全てが終了するまで繰り返す。

【0077】[第6の実施例] 図12は、本発明の第6の実施例のユーザ処理装置の構成を示す。同図において、図3と同一構成部分には、同一符号を付し、その説明を省略する。なお、本実施例は、図3の構成と同様である。

【0078】図12において、ユーザ処理装置100は、図3の構成に、復号部130で復号された命令を格納する復号済ソフトウェア格納部180と、当該復号済ソフトウェア格納部180に格納されている命令を順次読み出して実行する実行部190が付加されたものである。

【0079】図13は、本発明の第6の実施例の動作を説明するための図である。

ステップ601) ユーザ処理装置100において、予め命令部分が暗号化されたソフトウェア110を起動する。

ステップ602) ユーザ処理装置100は、ソフトウェア100をロードする。

【0080】ステップ603) ユーザ処理装置100の課金センタ送信部120は、ソフトウェアID、被課金者IDとを課金センタ200に送信する。

ステップ604) 課金センタ200の課金情報テーブル検索部230は、ユーザ処理装置100から受信したソフトウェアIDを用いて課金情報テーブル210を検索し、当該ソフトウェアの使用料と、第1の復号秘密鍵とを取得する。

【0081】ステップ605) ユーザ課金情報更新部240は、ユーザ処理装置100から受信した被課金者IDを用いてユーザ情報テーブル220を検索し、被課金者のユーザ課金情報を課金情報テーブル210から取得したソフトウェア使用料で更新する。

【0082】ステップ606) ユーザ処理装置送信部250は、課金情報テーブル検索部230から取得した第1の復号秘密鍵をユーザ処理装置100に送信する。

ステップ607) ユーザ処理装置100の復号部130は、課金センタ200から受信した第1の復号秘密鍵を用いて、ソフトウェアの全部または、一部の暗号化されている領域を復号する。

【0083】ステップ608) 復号部130は、復号したソフトウェアを復号済ソフトウェア格納部180に格納する。

ステップ609) 実行部190は、復号済ソフトウェア格納部180にアクセスし、復号されたソフトウェアを実行する。

【0084】[第7の実施例] 本実施例における課金情報テーブル210は、ソフトウェアID、機能に対応した機能ID、機能に対応した使用量と、機能に対応し、暗号化されているソフトウェアの全部又は一部の領域として復号するための第4の復号・秘密鍵を含むもの構

成である。第4の復号・秘密鍵は、ユーザ処理装置100に送信され、ソフトウェア110を復号するための鍵である。

【0085】図14は、本発明の第7の実施例の動作を説明するための図である。

ステップ701) ユーザ処理装置100は、予め機能毎に異なる秘密鍵を用いて暗号化されたソフトウェアを起動する。

ステップ702) 起動したソフトウェアをメモリ上にロードする。

【0086】ステップ703) ユーザ処理装置100の課金センタ送信部120は、実行しようとする機能の機能ID(機能A)と、ソフトウェアIDと、被課金者IDとを課金センタ200に送信する。

ステップ704) 課金センタ200の課金情報テーブル検索部230は、ユーザ処理装置から受信したソフトウェアIDと、機能IDとを用いて、課金情報テーブル210を検索し、当該機能の使用料と、第4の復号秘密鍵を取得する。

【0087】ステップ705) ユーザ課金情報更新部240は、課金情報テーブル検索部230により取得された機能使用料でユーザ情報テーブル220を更新する。

ステップ706) ユーザ処理装置送信部250は、課金情報テーブル210から取得した第1の復号秘密鍵をユーザ処理装置100に送信する。

【0088】ステップ707) ユーザ処理装置100は、課金センタ200から受信した第1の復号秘密鍵を用いて、当該機能の全部または、一部の暗号化されているソフトウェアの領域を復号して実行する。上記の手順を、当該ソフトウェアを使用してユーザが必要とする処理が終了するまで、機能の単位で繰り返す。ステップ708以降は、ユーザ処理装置100から機能IDとして“機能B”を課金センタ200に送信して、上記のステップ704～ステップ707と同様の処理を繰り返すものである。

【0089】なお、上記の各実施例において、ユーザ課金情報としては、前納方式、後納方式、累積課金方式、明細課金方式及びクレジット支払い方式のいずれにも適用可能である。また、上記の各実施例において、ソフトウェアをプログラムとして説明しているが、この例に限定されることなく、プログラムに留まらず、音声情報、映像除法、画像情報、テキスト情報を含む全てのデジタル情報に対して適用可能である。

【0090】なお、本発明は、上記の実施例に限定されることなく、特許請求の範囲内で種々変更・応用が可能である。

【0091】

【発明の効果】上述のように、本発明のソフトウェア課金方法及びシステムによれば、どの時点においても暗号

化されている部分を含まないソフトウェアが、メモリ及びディスク等の記憶媒体上に存在しないため、ソフトウェアの反復使用を確実に阻止することができ、ソフトウェアの使用の都度、確実に使用料を徴収することが可能となるため、ユーザは必要な機能のみを安価な使用料で使用する事が可能となる。

【0092】また、ソフトウェアの暗号化に用いる秘密鍵の個数と暗号化の範囲を選択することにより、起動するソフトウェアの単位で課金することも、起動するソフトウェア内の機能群単位に課金することも可能となる。また、使用料前払い、または、使用限度額に基づくクレジットを課金センタに登録して使用料残高を管理することにより、使用料の徴収漏れを防止することが可能となる。

【0093】また、ユーザ処理装置から課金センタに送信する時に添付した、乱数と課金センタからユーザ処理装置に送信する時に添付された乱数との一致を検証することにより、課金センタからユーザ処理装置に送信された情報を横取りすることによるソフトウェアの不正使用を防止することが可能となる。

【0094】また、課金センタからユーザ処理装置に送信において、公開暗号方式を利用し、署名を添付することにより、他人の被課金者IDを使用したソフトウェアの不正使用を防止することが可能となる。

【図面の簡単な説明】

【図1】本発明の原理を説明するための図である。

【図2】本発明の原理構成図である。

【図3】本発明のシステム構成図である。

【図4】本発明の第1の実施例の動作を説明するための図である。

【図5】本発明の第2の実施例のシステム構成図である。

【図6】本発明の第2の実施例の動作を説明するための図である。

【図7】本発明の第3の実施例の動作を説明するための図である。

【図8】本発明の第4の実施例のシステム構成図である。

【図9】本発明の第4の実施例のユーザ課金情報更新部の構成図である。

【図10】本発明の第4の実施例の動作を説明するための図である。

【図11】本発明の第5の実施例の動作を説明するための図である。

【図12】本発明の第6の実施例のユーザ処理装置の構成図である。

【図13】本発明の第6の実施例の動作を説明するための図である。

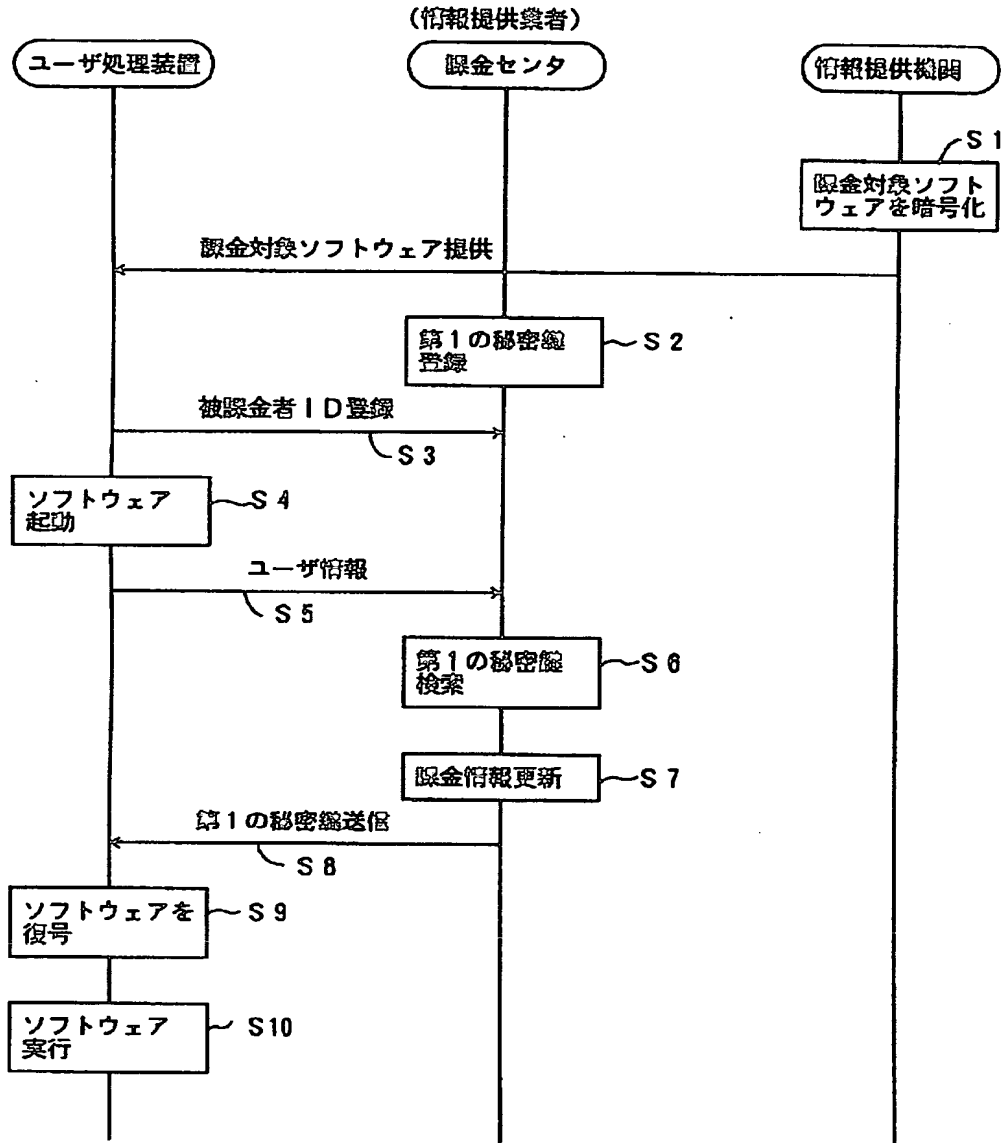
【図14】本発明の第7の実施例の動作を説明するための図である。

【符号の説明】

100	ユーザ処理装置
101	ID登録手段
110	ソフトウェア
120	課金センタ送信部、使用通知手段
130	復号部、第1の復号・秘密手段
140	乱数生成部
150	比較部
160	第3の秘密鍵保持部
170	署名生成部
180	復号済ソフトウェア格納部
190	実行部
200	課金センタ
201	第1の暗号化手段
202	ソフトウェア提供手段
210	課金情報テーブル
220	ユーザ情報テーブル
230	課金情報テーブル検索部
240	ユーザ課金情報更新部、課金手段
241	テーブル検索部
242	署名復号部
243	比較部
244	テーブル更新部
250	ユーザ処理装置送信部、復号鍵送信手段
260	乱数受信部

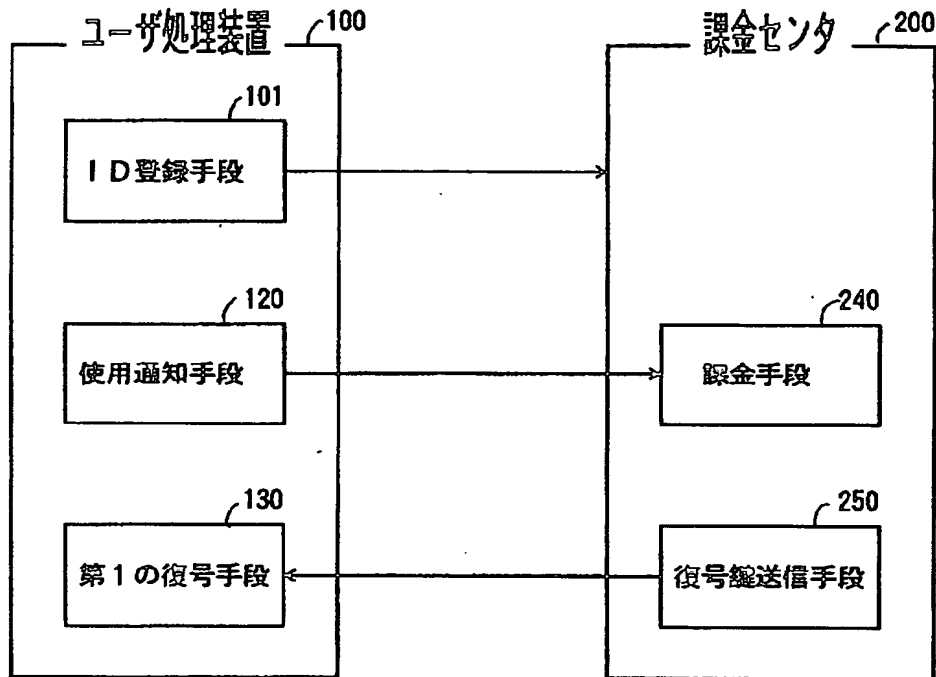
【図1】

本発明の原理を説明するための図



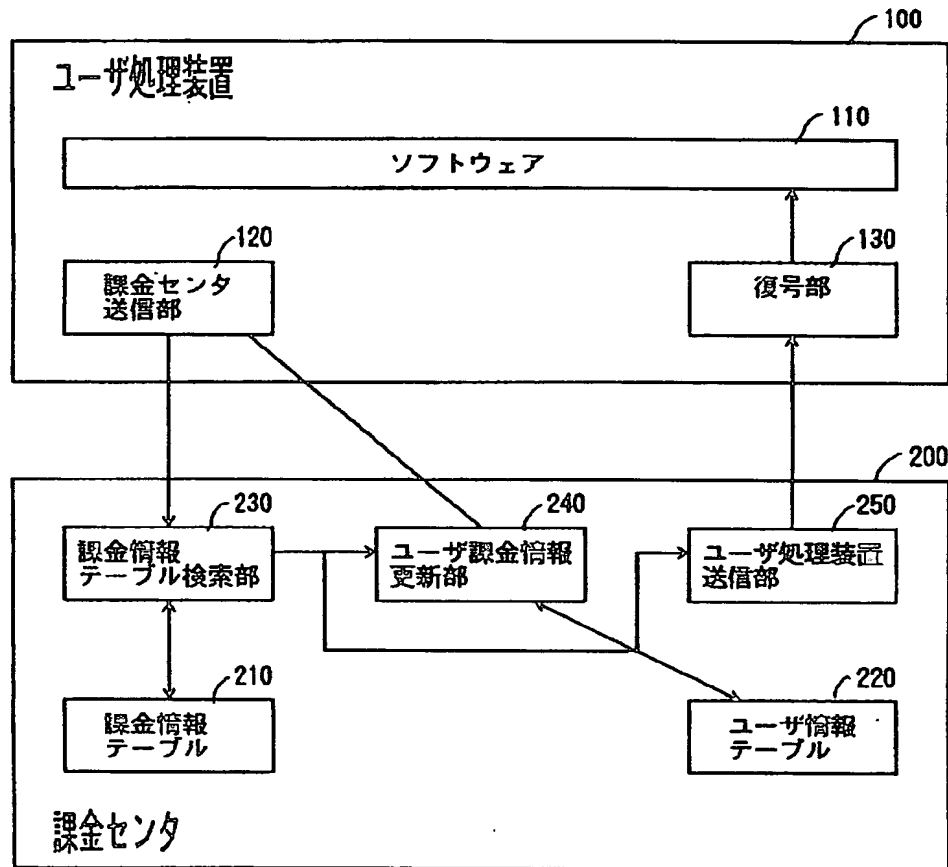
【図 2】

本発明の原理構成図



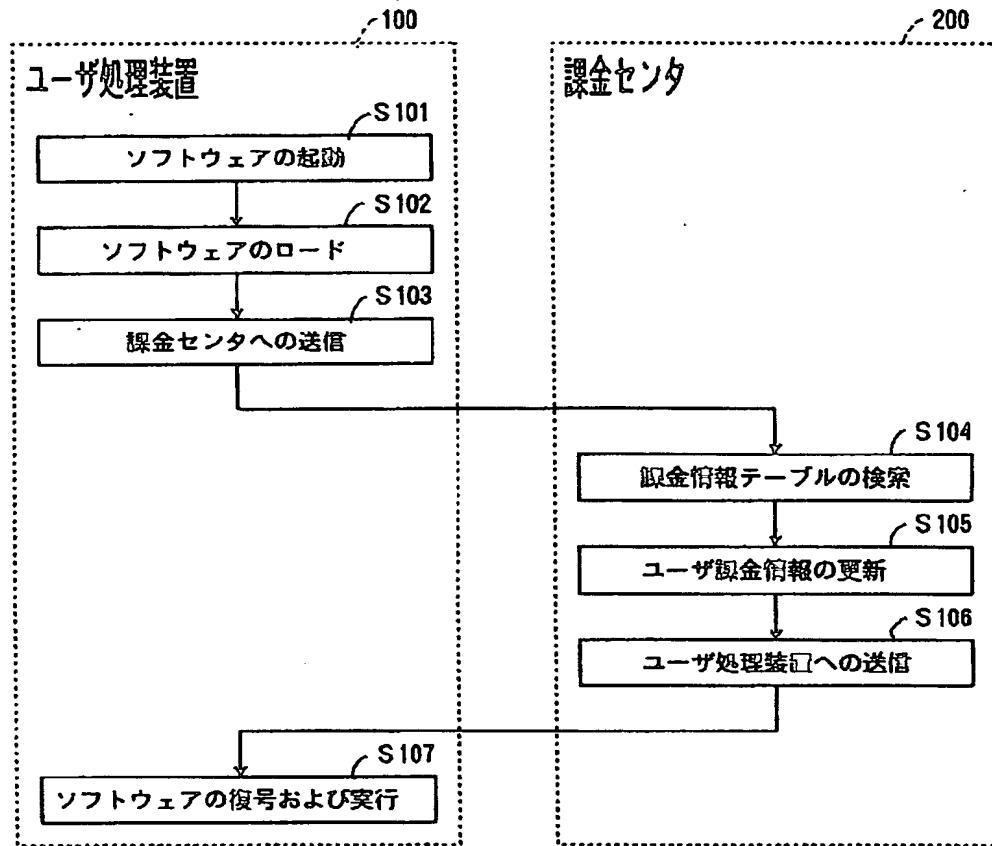
【図3】

本発明のシステム構成図



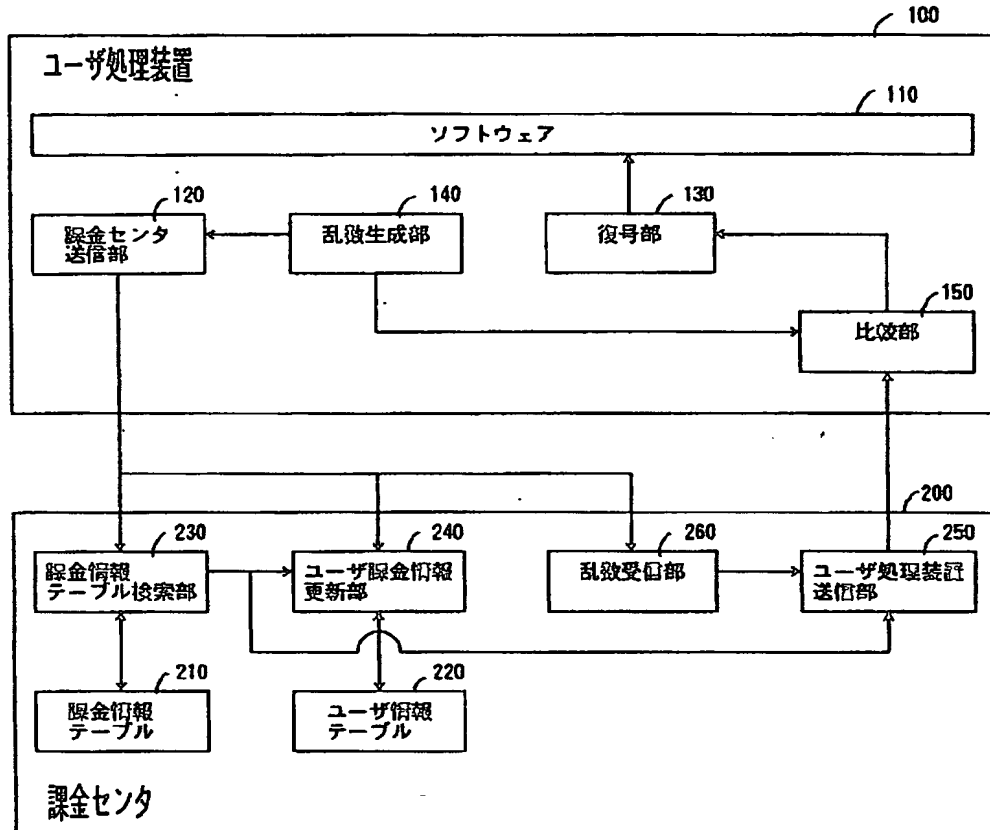
【図4】

本発明の第1の実施例の動作を説明するための図



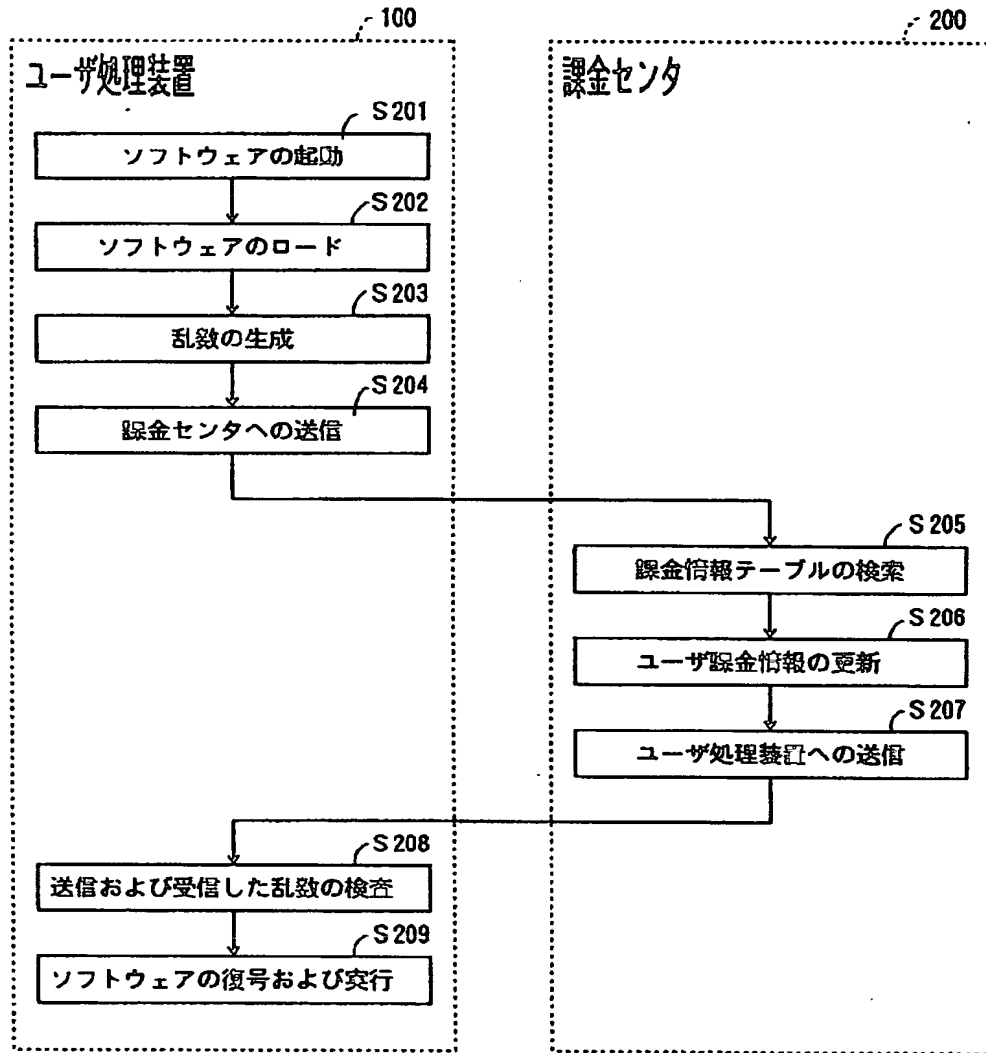
【図5】

本発明の第2の実施例のシステム構成図



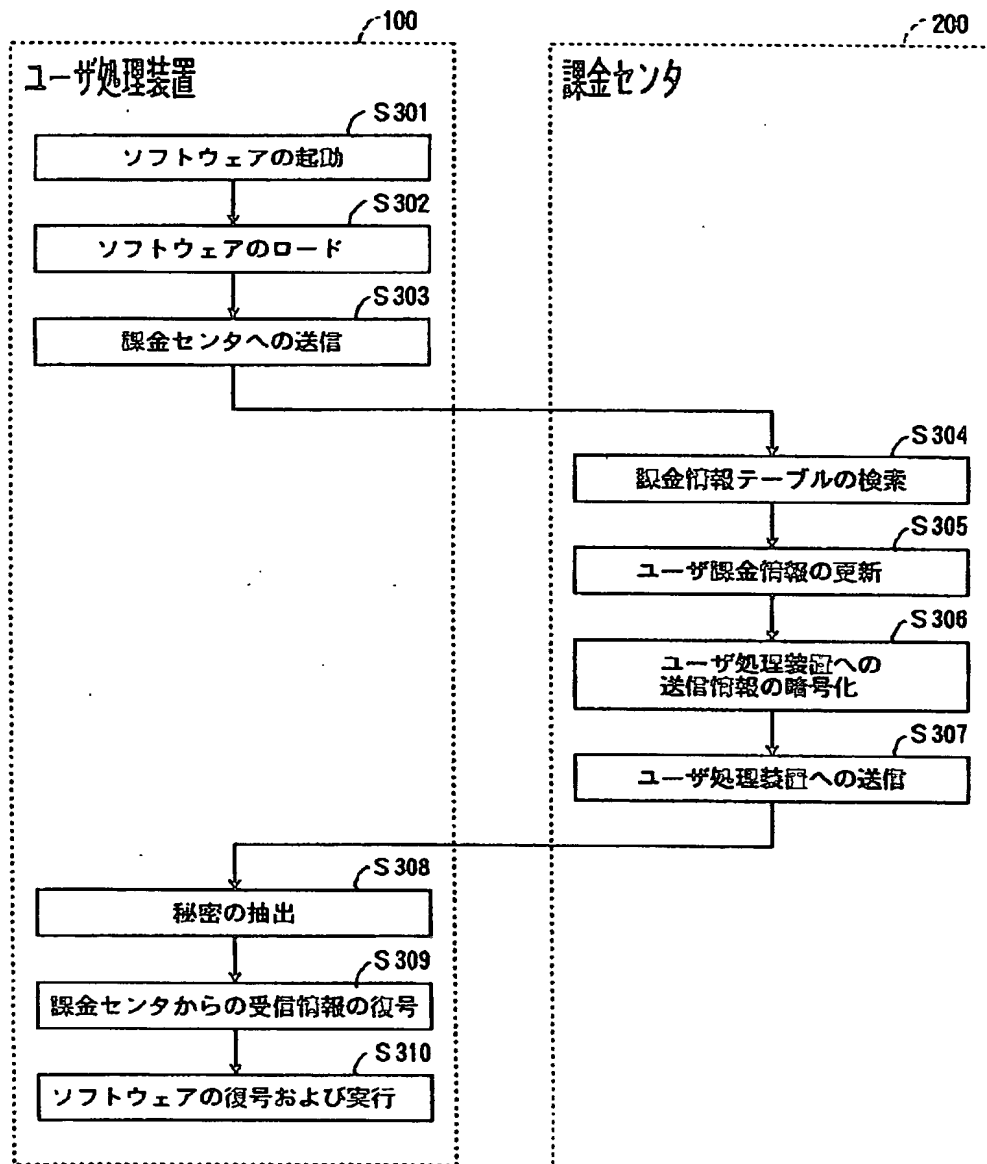
【図6】

本発明の第2の実施例の動作を説明するための図



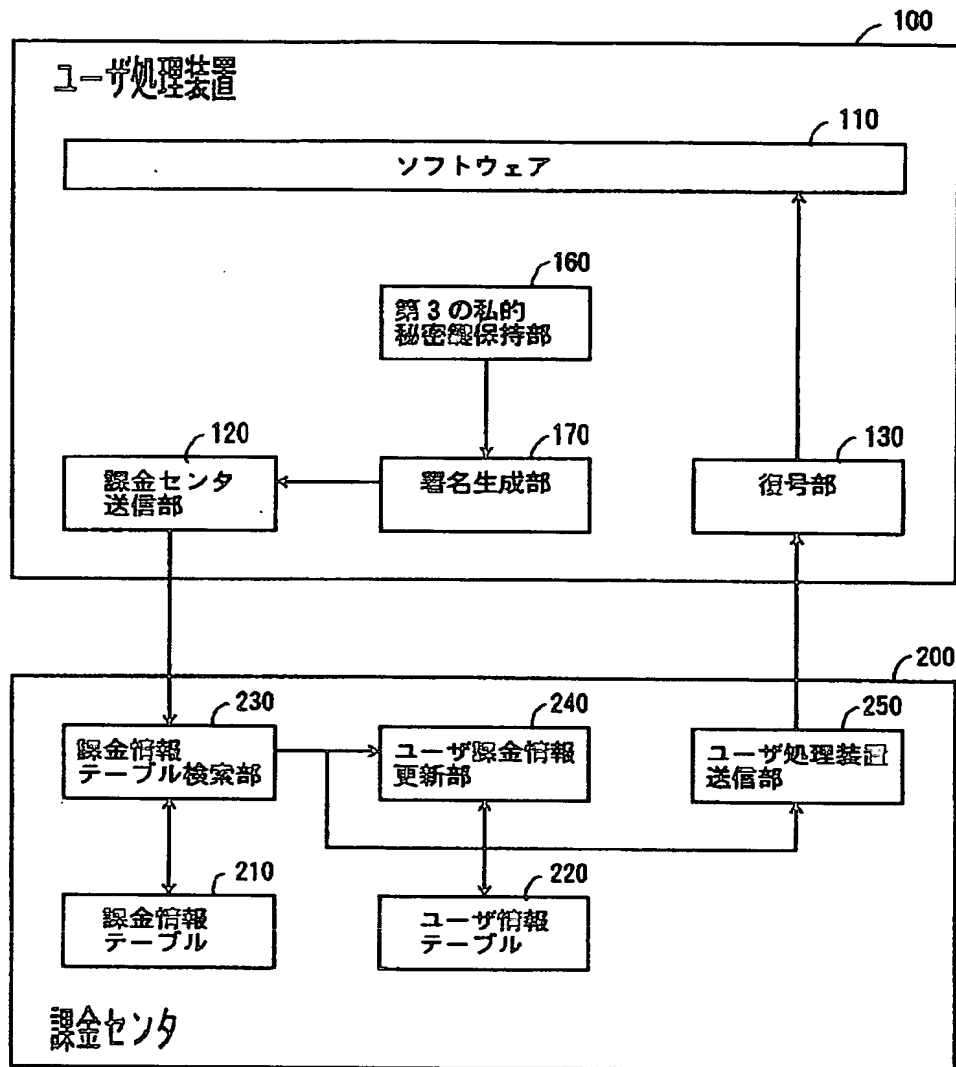
【図 7】

本発明の第 3 の実施例の動作を説明するための図



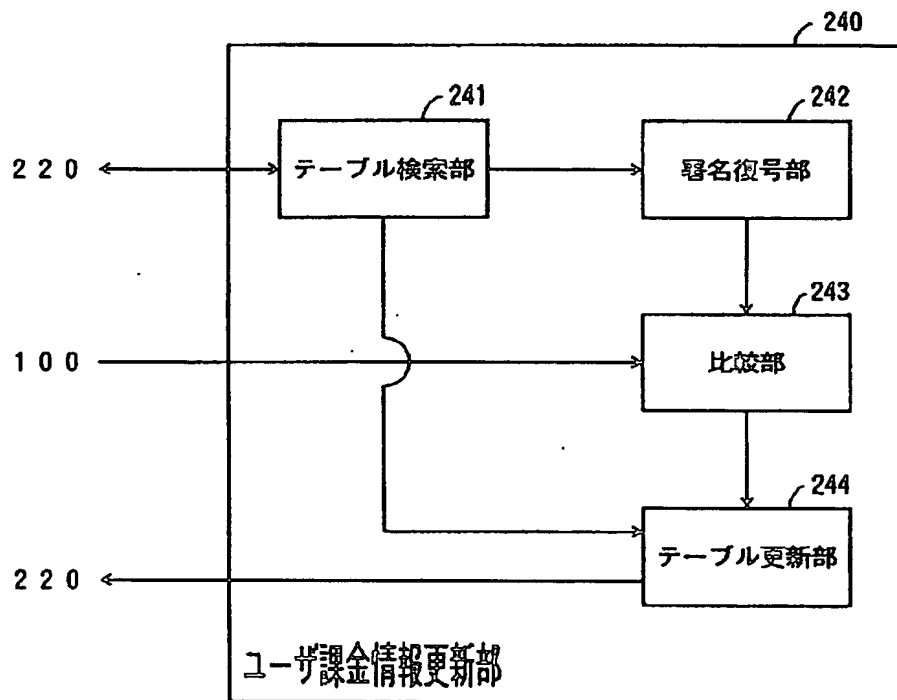
【図8】

本発明の第4の実施例のシステム構成図



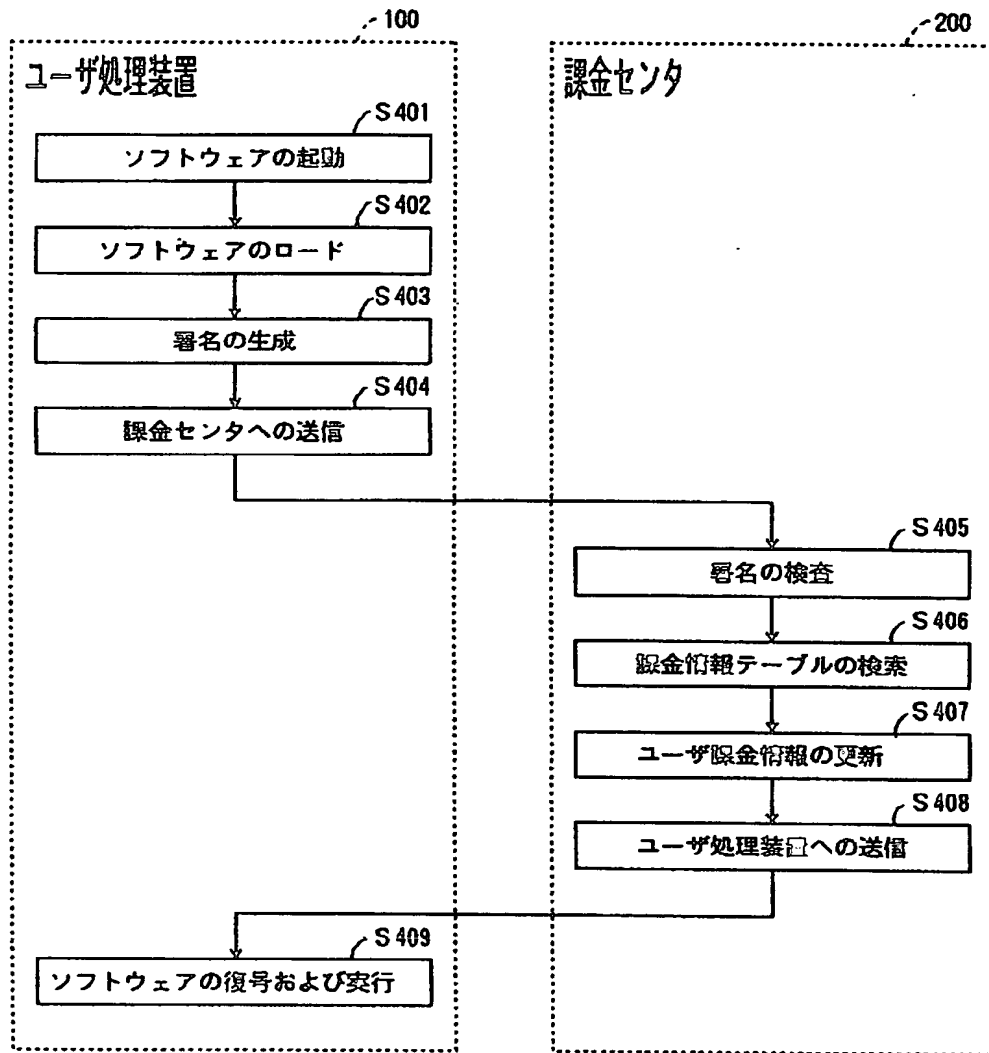
【図 9】

本発明の第 4 の実施例のユーザ課金情報更新部の構成図



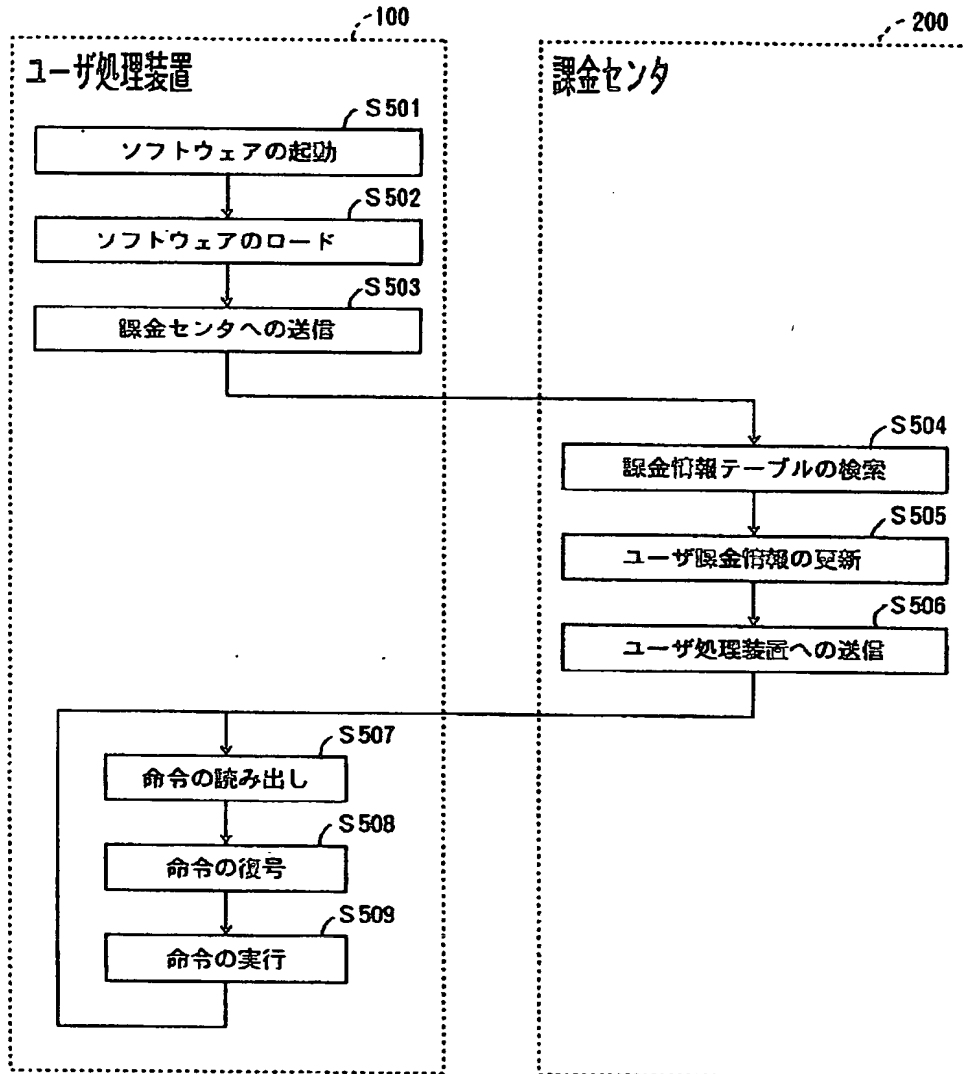
【図10】

本発明の第4の実施例の動作を説明するための図



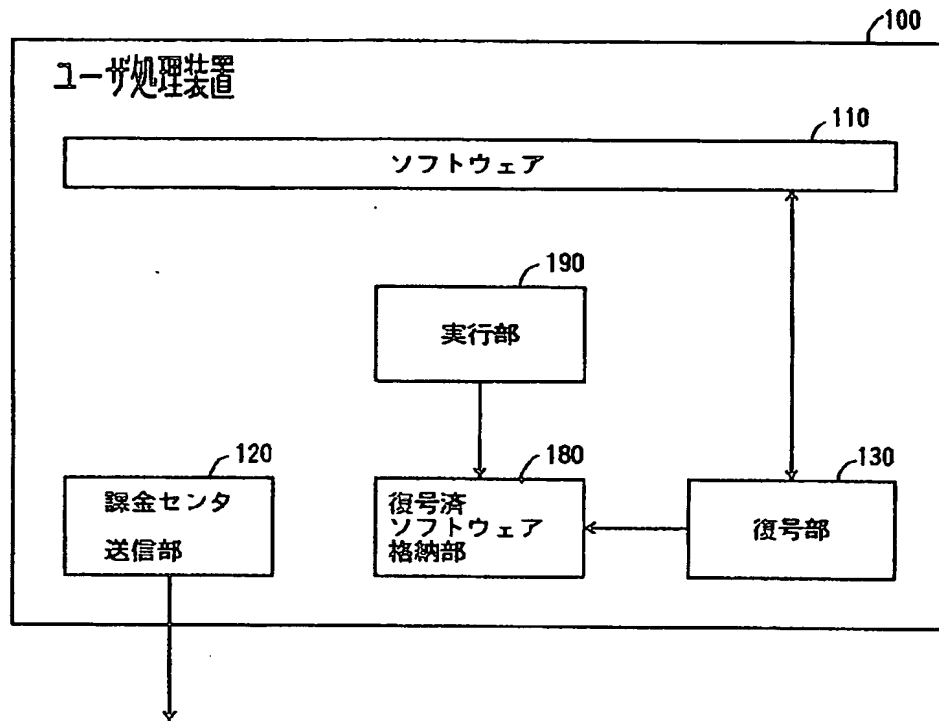
【図11】

本発明の第5の実施例の動作を説明するための図



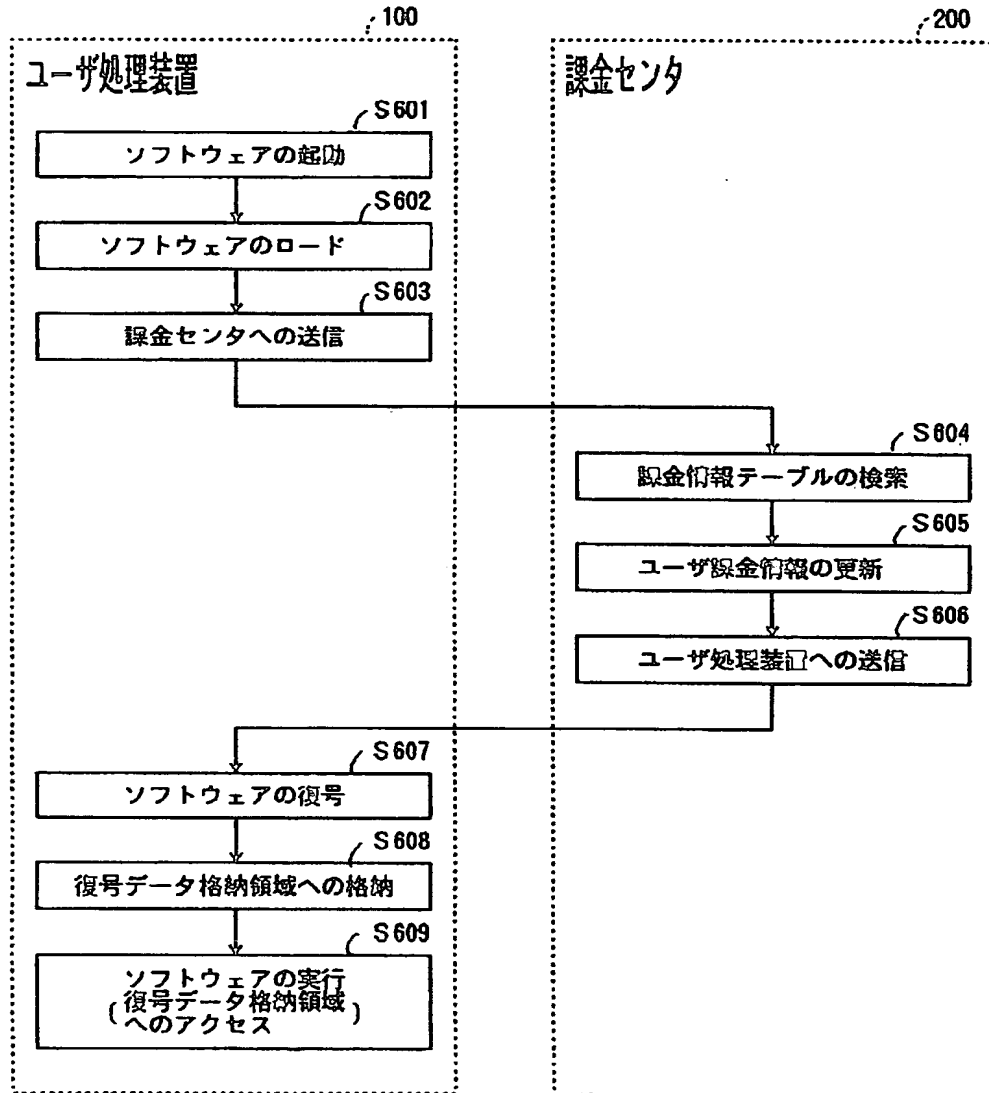
【図12】

本発明の第6の実施例のユーザ処理装置の構成図



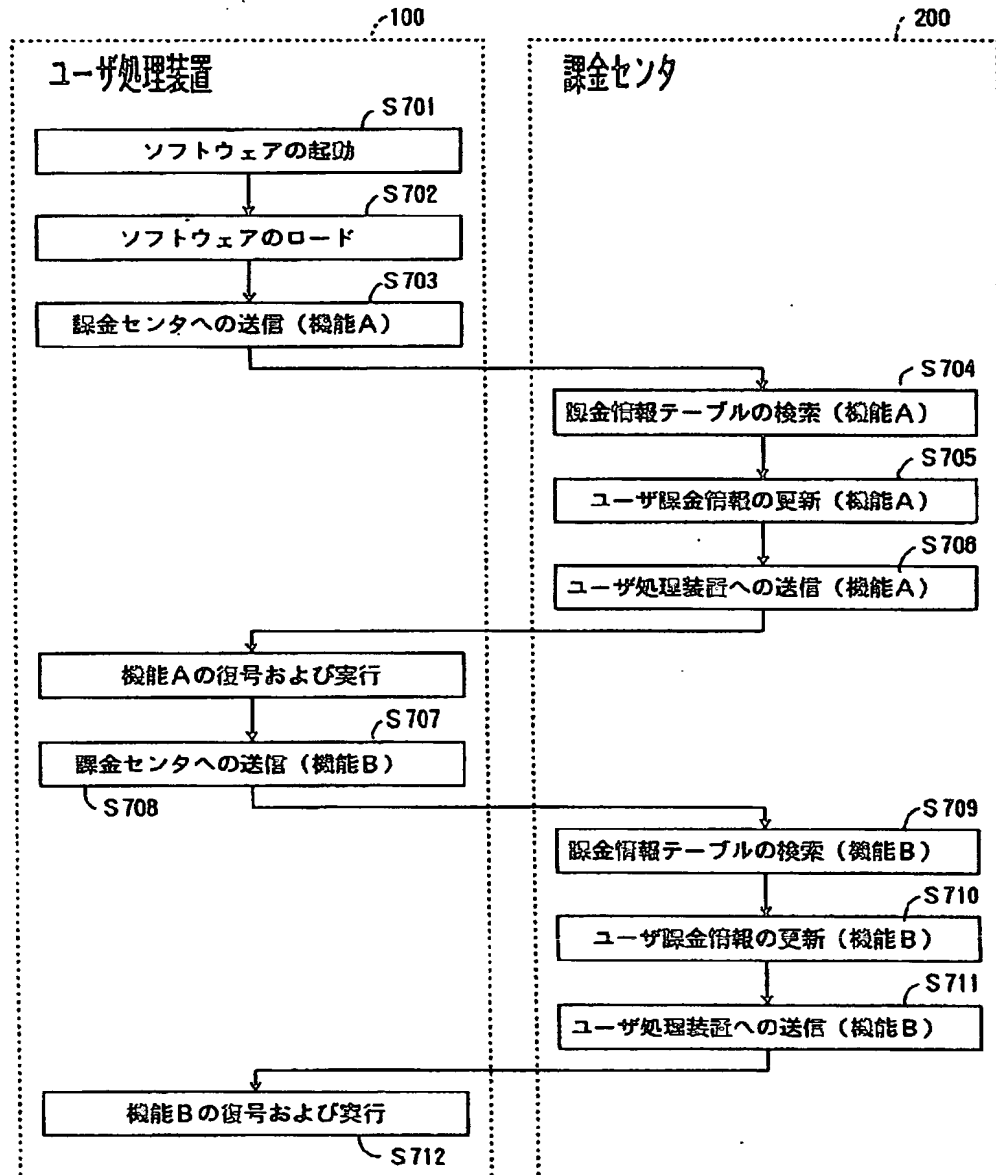
【図13】

本発明の第6の実施例の動作を説明するための図



【図 14】

本発明の第 7 の実施例の動作を説明するための図



フロントページの続き

(51) Int. Cl. ⁶

G 0 9 C 1/00

識別記号

6 4 0

庁内整理番号

7259-5 J

F I

G 0 9 C 1/00

技術表示箇所

6 4 0 B

6 4 0 E

6 6 0 Z

6 6 0 D

6 6 0

7259-5 J

7259-5 J